AF/2132
$ ZW

Docket No. AUS990150US1

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Rich et al.** §
§ Group Art Unit: **2132**
Serial No. **09/464,854** §
§ Examiner: **Gurshman, Grigory**
Filed: **December 16, 1999** §
§
For: **Notification of Modifications to a Trusted Computing Base** §
§

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certificate of Mailing Under 37 C.F.R. § 1.8(a)

I hereby certify this correspondence is being deposited with the United States Postal Service as First Class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on December 28, 2004.

By: Amelia C. Turner
Amelia C. Turner

APPEAL BRIEF (37 C.F.R. 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on September 29, 2004.

The fees required under § 41.20(B)(2), and any required petition for extension of time for filing this brief and fees therefore, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

REAL PARTY IN INTEREST

The real party in interest in this appeal is the following party: International Business Machines Corporation.

RELATED APPEALS AND INTERFERENCES

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interferences.

STATUS OF CLAIMS

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-23

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims canceled: NONE
2. Claims withdrawn from consideration but not canceled: NONE
3. Claims pending: 1-23
4. Claims allowed: NONE
5. Claims rejected: 1-23

C. CLAIMS ON APPEAL

The claims on appeal are: 1-23

STATUS OF AMENDMENTS

No amendments have been submitted since the final office action was received.

SUMMARY OF CLAIMED SUBJECT MATTER

A. CLAIM 1 – INDEPENDENT

The subject matter of claim 1 is directed to a method for notifying a central authority of changes to a trusted computing installation, summarized at page 4, lines 3-7. **Figure 1** depicts a block diagram of a computer that supports the innovative architecture and is discussed on page 8, lines 6-18, while **Figure 3** depicts the steps of the method and is discussed in the section from page 14, line5 through page 17, line 4. The three steps in the claim comprise (a) determining that a user has made a security modification to a portion of the trusted computing installation (step **44**), (b) determining that a notification should be sent because the security modification is a predetermined event indicative of an attempt to circumvent a security mechanism (step **48**), and (c) responsive to making the determination, sending the central authority a notification of the security modification (step **50**).

B. CLAIM 2 – DEPENDENT

The subject matter of claim 2 is directed to defining the predetermined even of claim 1, which is defined as being in the group consisting of a failed applet signature verification, an addition of a certificate in a certificate database and a modification of a certificate in a certificate database, discussed on page 2, lines 6-25 and in the section from page 15, line 22 through page 17, line 4.

C. CLAIM 3 – DEPENDENT

The subject matter of claim 3 is directed to defining the predetermined event of claim 1 as being a Java applet wishing to run with higher privileges and comprising the additional steps of verifying a signature of the Java applet; responsive to a failed verification of the signature, running the applet as untrusted; and sending the central authority a notification of the failed verification, discussed in the section from page 15, line 22 through page 16, line 15.

D. CLAIM 6 – DEPENDENT

The subject matter of claim 6 is directed to define the security modification as allowing un-trusted code to run, discussed in the section from page 13, line 15 through page 14, line 4.

E. CLAIM 9 – INDEPENDENT

The subject matter of claim 9 is directed to a method of notifying a central authority of changes to a trusted computing installation, as summarized on page 4, lines 3-7. **Figure 4** depicts a high level flowchart illustrating the operation f the security notification manager abstract class and is discussed from page 19, line 8 through page 21, line 32. **Figure 5** illustrates the mechanism of the security notification manager abstract class **70** and instances **72a** – **72n** that extend the base class and is discussed from page 21, line 33 through page 22, line 8. Again, **Figure 1** depicts a block diagram of a computer that supports the innovative architecture and is discussed on page 8, lines 6-18, while **Figure 3** depicts the steps of the method and is discussed in the section from page 14, line5 through page 17, line 4. In claim 9, the recited steps comprise: (a) determining that a user has made a security modification to a portion of the trusted computing installation under user control (step **44**), invoking a security notification manager class (step **46,** which is expanded in steps **52** through **62,** instantiating the security manager class with an instance (step 62) that determines that the security modification is a notification event if the security modification is a predetermined event indicative of an attempt to circumvent a security mechanism of the trusted computing installation (step 48), and issuing a notification (step 50).

F. CLAIM 12 –DEPENDENT

The subject matter of claim 12 is directed to defining that the location of the security modification is in the applet signature verification routine, discussed in the section from page 15, line 22 through page 16, line 15.

G. CLAIM 14 – INDEPENDENT

The subject matter of claim 14 is directed to a method for notifying a central authority of changes to a trusted computing installation and relies on the same disclosure as claim 9. In claim 14, the recited steps are (a) upon a given security modification, invoking a security notification manager class (step **46/52**), (b) extending the security notification manager class with one of a set of instances (step **62**), wherein a given instance determines that the security modification is a notification event if the security modification is a predetermined event indicative of an attempt to circumvent a security mechanism of the trusted computing installation (step **48**), and sending the central authority a notification of the security modification (step **50**).

H. CLAIM 15– INDEPENDENT

The subject matter of claim 15 is directed to a computer program product for notifying an authority of changes to a trusted computing installation and is substantially a computer program counterpart to method claim 14.

I. CLAIM 18– INDEPENDENT

The subject matter of claim 18 is directed to a computer program product for notifying an authority of changes to a trusted computing installation and is substantially a computer program counterpart to method claim 9.

J. CLAIM 19– INDEPENDENT

The subject matter of claim 19 is directed to a trusted computing base, shown in **Figure 1** and discussed on page 8, lines 6-18. This claim is substantially an apparatus claim counterpart to dependent method claim 6.

K. CLAIM 22– INDEPENDENT

The subject matter of claim 22 is directed to a notification service for a trusted computing installation. The computer is shown in Figure 1 and is discussed on page 8, lines 6-18, comprising. The mechanism of the service is shown in **Figure 5**, discussed in the section from page 21, line 33 through page 23, line 7. The service contains a framework, i.e. the security manager abstract class **70**, into which class instances that implement the rules and send notifications can be plugged, see page 23, lines 8-20

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. **GROUND OF REJECTION 1 (Claims 1, 4-6, 8, 22, and 23)** Claims 1, 4-6, 8, 22, and 23 stand rejected under 35 U.S.C. § 102 as anticipated over *O'Toole* (6,279,112).

B. **GROUND OF REJECTION 2 (Claims 9-11 and 13-21[1] 14,15,18, 19)** Claims 9-11 and 13-21[2] 14,15,18, 19 stand rejected under 35 U.S.C. § 103 as obvious over *O'Toole* in view of International Business Machine Corp (RD 414099A, hereinafter *IBMC*).

C. **GROUND OF REJECTION 3 (Claim 2)** Claim 2 stands rejected under 35 U.S.C. § 103 as obvious over *O'Toole* in view of *Renaud* (6,279,112).

D. **GROUND OF REJECTION 4 (Claims 3 and 12)** Claims 3 and 12 stand rejected under 35 U.S.C. § 103 as obvious over *O'Toole* in view of *IBMC* and *Renaud.*

[1] While this rejection does not specifically recite claim 7, the discussion refers to this claim; it is believed that the rejection is intended to include claims 7, 9-11, and 13-21.

[2] While this rejection does not specifically recite claim 7, the discussion refers to this claim; it is believed that the rejection is intended to include claims 7, 9-11, and 13-21.

ARGUMENTS

A. GROUND OF REJECTION 1 (Claims 1, 4-6, 8, 22, and 23)

Claims 1, 4, 5, 8, 22, and 23

Claims 1, 4-6, 8, 22, and 23 have been rejected under 35 U.S.C. § 102(e) as being anticipated by *O'Toole, Jr. et al.* (U.S. Patent Number 6,279,112), hereinafter referred to as *O'Toole*. This rejection is respectfully traversed.

Representative claim 1 reads as follows,

> 1. A method for notifying a central authority of changes to a trusted computing installation, comprising the steps of:
>
> determining that a user has made a security modification to a portion of the trusted computing installation under user control;
>
> determining that the security modification is a notification event if the security modification is a predetermined event indicative of an attempt to circumvent a security mechanism of the trusted computing installation; and
>
> sending the central authority a notification of the security modification, in response to determining that the security modification is a notification event. (emphasis added)

Regarding claims 1 and 22, the office action states,

> Referring to the instant claims, O'Toole discloses control transfer of information in computer networks (see abstract and Fig. 1).
>
> O'Toole teaches that the client computer notifies the server computer (or the information source computer) that the access ticket was added to the access control list – see column 5, lines 23-30 and Fig 2, block 32. O'Toole teaches that client computer 200 also stores a client security profile 208 that specifies that certain information in client personal profile 206 should be disclosed to server computer 202 only to trusted servers or only upon authorization from the client user or both. A client "avatar" 210 located at client computer 200 acts as an agent for the user by controlling the release of information from client personal profile 206 to server computer 202 (see Fig. 5).
>
> Referring to claim 1, the limitation "determining that a user has made a security modification to a portion of the trusted computing installation" is met by adding the access ticket to the access control list of the channel object of the client computer (see Fig. 1 and Fig. 2, block 30). The limitation "determining that the security modification is a notification event of interest" is met by sending the central authority a notification of the security modification" is met by client computer notifying server computer that access ticket was added to access control list (see Fig. 2, block 32).

> Referring to claim 22, the limitation “a pluggable framework for receiving a set of notification objects …” is met by notification server (see block 16 in Fig. 2).[3]

Looking at the cited portions of *O'Toole*, we read in the abstract,

> The present invention relates to techniques for controlling transfers of information in computer networks. One technique involves transmitting from a server computer to a client computer a document containing a channel object corresponding to a communication service, and storing an access ticket that indicates that a user of the client computer permits the information source computer to communicate with the user over a specified channel. Another technique involves transmitting smart digital offers based on information such as coupons and purchasing histories stored at the computer receiving the offer. Another technique involves transmitting from a server computer to a client computer a request for a user's personal profile information, and activating a client avatar that compares the request for personal profile information with a security profile of the user limiting access to personal profile information. Another technique involves transmitting from a server computer to a client computer a document containing an embedded link, activating the embedded link at the client computer and recording activation of the embedded link in a metering log.

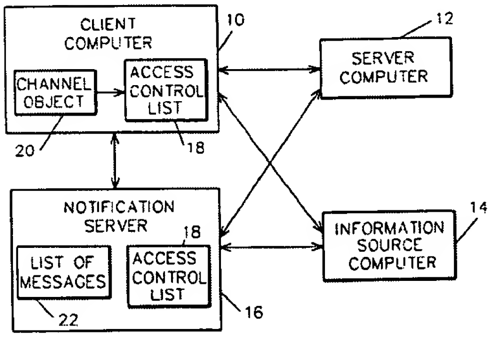

FIG. 1

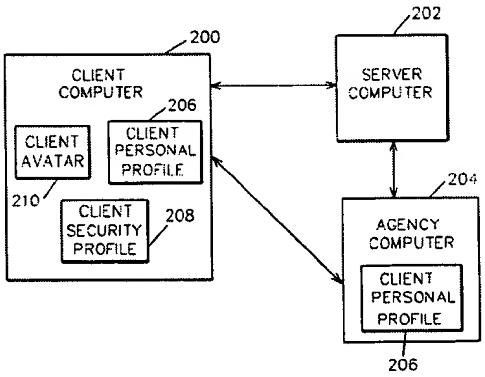

FIG. 5

Figure 5 of *O'Toole* is shown on the following page, while the referenced portion of the specification of *O'Toole* reads,

> Once the channel object has been activated, the client computer notifies the server computer (or the information source computer, or another computer) that the access ticket was added to the access control list (step 32) and the server computer (or the information source computer, or another computer) records in a persistent database the client's interest in the channel object and

[3] Office Action dated December 3, 2003, page 3.

> sends a confirmation to the client computer that the client's interest in the channel object has been recorded (step 34).[4]

A prior art reference anticipates the claimed invention under 35 U.S.C. § 102 only if every element of a claimed invention is identically shown in that single reference, arranged as they are in the claims. *In re Bond*, 910 F.2d 831, 832, 15 U.S.P.Q.2d 1566, 1567 (Fed. Cir. 1990). All limitations of the claimed invention must be considered when determining patentability. *In re Lowry*, 32 F.3d 1579, 1582, 32 U.S.P.Q.2d 1031, 1034 (Fed. Cir. 1994). Anticipation focuses on whether a claim reads on the product or process a prior art reference discloses, not on what the reference broadly teaches. *Kalman v. Kimberly-Clark Corp.*, 713 F.2d 760, 218 U.S.P.Q. 781 (Fed. Cir. 1983).

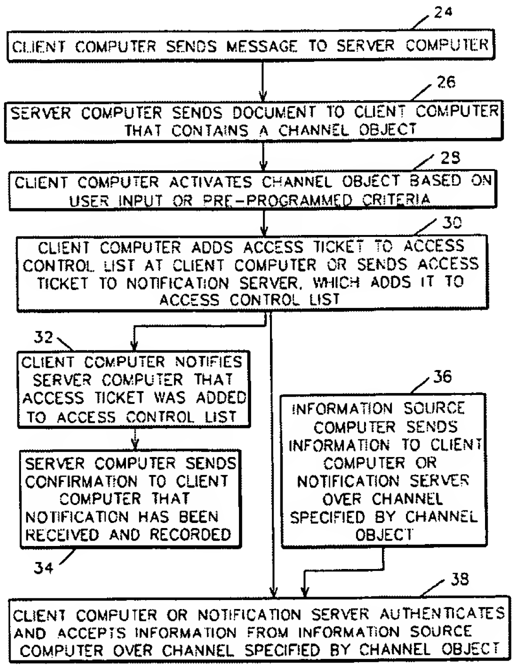
24
CLIENT COMPUTER SENDS MESSAGE TO SERVER COMPUTER
26
SERVER COMPUTER SENDS DOCUMENT TO CLIENT COMPUTER THAT CONTAINS A CHANNEL OBJECT
28
CLIENT COMPUTER ACTIVATES CHANNEL OBJECT BASED ON USER INPUT OR PRE-PROGRAMMED CRITERIA
30
CLIENT COMPUTER ADDS ACCESS TICKET TO ACCESS CONTROL LIST AT CLIENT COMPUTER OR SENDS ACCESS TICKET TO NOTIFICATION SERVER, WHICH ADDS IT TO ACCESS CONTROL LIST
32
CLIENT COMPUTER NOTIFIES SERVER COMPUTER THAT ACCESS TICKET WAS ADDED TO ACCESS CONTROL LIST
SERVER COMPUTER SENDS CONFIRMATION TO CLIENT COMPUTER THAT NOTIFICATION HAS BEEN RECEIVED AND RECORDED
34
36
INFORMATION SOURCE COMPUTER SENDS INFORMATION TO CLIENT COMPUTER OR NOTIFICATION SERVER OVER CHANNEL SPECIFIED BY CHANNEL OBJECT
38
CLIENT COMPUTER OR NOTIFICATION SERVER AUTHENTICATES AND ACCEPTS INFORMATION FROM INFORMATION SOURCE COMPUTER OVER CHANNEL SPECIFIED BY CHANNEL OBJECT

FIG. 2

Applicant respectfully submits that *O'Toole* does not identically show every element of the claimed invention arranged as they are in the claims. In the first response, mailed 03/03/04, applicant argued that *O'Toole* does not teach determining that a user has made a security modification that is indicative of an attempt to circumvent a security mechanism to the trusted computer installation, noting that,

[4] O'Toole at column 5, lines 23-30.

> *O'Toole* is directed towards methods for controlling transfers of information in computer networks ... One of the methods of *O'Toole* involves transmitting a document containing a channel object corresponding to a communication service from a server computer to a client computer, and storing an access ticket that indicates that a user of the client computer permits the information source computer to communicate with the user over a specified channel. ...
>
> While *O'Toole* teaches to send the access ticket to the notification server, there is nothing in the sending of the access ticket to the notification server that teaches or even suggests that a security modification is a notification event if the security modification is a predetermined event indicative of an attempt to circumvent a security mechanism of a trusted computing installation. To the contrary, the access ticket of *O'Toole* is the security mechanism that provides the security necessary for the communication service from a server computer to a client computer. There is no circumvention of security mechanisms being performed by the addition of the access ticket to the access control list.[5]

In reply to applicant's earlier arguments, the final rejection responds,

> ... using broad but reasonable interpretation, one of ordinary skill in the art would have equated a security modification with adding the access ticket to the access control list of the computer. ... Examiner also points out that the addition of a new access ticket to the access control list is a circumvention of the security mechanism as this action can potentially allow an unauthorized user to access the trusted compute[r] installation.[6]

It is respectfully asserted that the examiner is reading something into *O'Toole* that is not presented by this patent. While *O'Toole* does show modifying an access list, which the rejection asserts is a circumvention of security mechanisms, *O'Toole* also clearly discusses the means by which this system prevents unauthorized intrusions into the user's computer. Not only does the access list provide limited access to outside computers; other protections are also provided. *O'Toole* discloses,

> The information source computer ... asynchronously sends information to the client computer or the notification server (step **36**) over the channel specified by the channel object. The information includes an identification of its supplier and is signed using a private key of a public/private key pair. The client computer of the notification server accepts the information based on the presence of the appropriate access ticket in the access control list (step **38**) corresponding to the supplier of the information and based on the client computer's use of the public key contained in the access ticket to ensure authenticity of the information.[7] ...

[5] Response to first office action, pages 10-11.

[6] Final office action of 06/30/2004.

[7] O'Toole, column 5, lines 32-45, underlining added.

> Referring to FIGS. **4A** and **4B**, in operation of the network-based system of FIG. **3**, the coupon-providing server sends a document to the client computer containing an embedded digital coupon (step **112**). The coupon may be an executable program or program fragment expressed in machine-executable form, such as an ActiveX applet, and protected against unauthorized tampering by means of an authenticator such as a digital signature or MAC code (Message Authentication Code), or the coupon may be a digitally signed set of inputs to a program already residing at the client computer. The coupon contains a set of restrictions such as an expiration date, a product code or item number, and a discount amount. Alternatively, the coupon may simply contain a coded number that can be understood by the smart digital offer object described below.[8]

As shown by the excerpts above from *O'Toole*, this patent is very concerned that adding the disclosed access to the client's computer does not open the user to security problems. *O'Toole* appears to disclose that any information that is received as a result of the disclosed addition to the access list is carefully controlled by the use of digitally signed programs, public/private keys, etc. It is respectfully submitted that unless the examiner can show that *O'Toole* leaves avenues open for unwanted intrusions, it is submitted that *O'Toole*'s action of adding an access key to an access list and informing an authority that this has been done does not meet the requirements of an anticipation rejection.

In view of the above, Applicants respectfully submit that *O'Toole* does not teach each and every feature of representative claim 1 as is required under 35 U.S.C. § 102(a). Accordingly, Applicants respectfully request the Board of Appeals to withdraw the rejection of claims 1, 4-6 and 22-23 under 35 U.S.C. § 102(a).

Claim 6

It is further noted that claim 6 contains additional subject matter that was not addressed in the final office action, after amendments were made to this claim. This claim is argued separately from the other claims in this group, because it is submitted that the particular recitations of this claim deserve separate consideration. Claim 6, in addition to the recitations of its parent claim, recites,

> 6. The method as described in Claim 1 wherein the security modification is to allow untrusted code to run in the trusted computing installation.

[8] O'Toole, column 6, lines 53-67, underlining added.

Attention is drawn to the rejection of claim 6 in the final office action, which states,

> "referring to claims 5 and 6, it is inherent to send notifications in the form of Simple Network Management Protocol (SNMP) alerts or in the form of an e-mail messages or screen messages"[9].

The rejection does not refer to the claim as it was amended in applicants' response to the first office action, but rather to its form at the time the application was filed. It appears that no comment has been made in the office action regarding the current limitation that "untrusted code" is allowed "to run in the trusted computing installation". Thus, the office action has not made a case for the rejection of this claim and this claim should be allowed.

However, applicant's arguments regarding claim 6 do not rely solely on the fact that the amendments to this claim appear to have been overlooked in the final rejection. Rather, applicants note that a major question raised with regard to claim 1 is whether or not the prior art discloses that, "the security modification is a predetermined event indicative of an attempt to circumvent a security mechanism of the trusted computing installation". Claim 6 clearly identifies that what defines an attempt to circumvent security is "allow[ing] untrusted code to run in the trusted computing installation". As discussed above, *O'Toole* repeatedly shows how this patent ensures that there is no security breach caused by adding the access ticket to the access list. *O'Toole* is not allowing untrusted code to run, but clearly requires the use of signed, and therefore trusted, applications and the use of public/private codes. Thus, it is asserted that *O'Toole* does not show the limitations of claim 6.

Furthermore, *O'Toole* does not teach, suggest, or give any incentive to make the needed changes to reach the presently claimed invention, in any of the claims discussed above. Absent the Examiner pointing out some teaching or incentive to modify *O'Toole* to meet the claimed invention, one of ordinary skill in the art would not be led to modify *O'Toole* to reach the present invention when the reference is examined as a whole. Absent some teaching, suggestion, or incentive to modify *O'Toole* in this manner, the presently claimed invention can be reached only through an improper use of hindsight using the applicants' disclosure as a template to make the necessary changes to reach the claimed invention. The Board of Appeals is requested to overturn this rejection.

[9] Final office action, item 16, page 6.

B. GROUND OF REJECTION 2 (Claims 7, 9-11, and 13-21

Claims 7, 9-11, 13-18, and 20-21

Claims 7, 9-11, and 13-21 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over *O'Toole* in view of *INT BUSINESS MACHINES CORP [IBMC]* (RD 414099A), hereinafter referred to as *IBMC*. This rejection is respectfully traversed.

Repeating the original rejection, the final Office Action states,

> Referring to the instant claims, O'Toole discloses control transfer of information in computer networks (see abstract and Fig. 1). O'Toole teaches that the client computer notifies the server computer (or the information source computer) that the access ticket was added to the access control list – see column 5, lines 23-30 and Fig. 2, block 32. O'Toole teaches that client computer 200 also stores a client security profile 208 that specifies that certain information in client personal profile 206 should be disclosed to server computer 202 only to trusted servers or only upon authorization from the client user or both. The limitation "determining that a user has made a security modification to a portion of the trusted computing installation" is met by adding the access ticket to the access control list of the channel object of the client computer (see Fig. 1 and Fig. 2, block 30). The limitation "determining that the security modification is a notification event of interest" is met by sending the access ticket to notification server (see Fig. 2, block 30). The limitation "sending the central authority a notification of the security modification" is met by client computer notifying server computer that access ticket was added to access control list (see Fig. 2, block 32). O'Toole, however, does not teach or suggest the use of a security modification manager class.
>
> Referring to the instant claims, INT BUSINESS MACHINE CORP (hereinafter IBMC) discloses a security environment for evaluating and executing Java applications (see abstract). IBMC teaches that the settings for each of the operation checks are defined by the JAVA security manager class (see page 2, basic-abstract). Therefore, at the time the invention was made it would have been obvious to one of ordinary skill in the art to determine that a security modification has been made to the computing installation of O'Toole and invoke a JAVA security manager class as taught in IBMC. One of ordinary skill in the art would have been motivated to determine that a security modification has been made to the computing installation and invoke a JAVA security manager class as taught in IBMC for defining the setting of the operation to be performed (see IBMC, page 2, basic abstract). The limitation "instantiating the security manager class" is met by parameters required for the application (see abstract).[10]

Claim 9, which is representative of this set of claims, reads as follows:

> 9. A method of notifying a central authority of changes to a trusted computing installation, comprising the steps of:
>
> determining that a user has made a security modification to a portion of the trusted computing installation under user control;
>
> invoking a security notification manager class;
>
> instantiating the security manager class with an instance that determines that the security modification is a notification event if the security modification is a predetermined event indicative of an attempt to circumvent a security mechanism of the trusted computing installation; and
>
> sending the central authority a notification of the security modification, in response to determining that the security modification is a notification event.
>
> (emphasis added)

It appears that *IBMC* has been added to the rejection of this group of claims to show a disclosure of a Java security manager class to the disclosure of *O'Toole*. The cited Derwent abstract for this document reads,

> The provision describes shield type program that allows user to create and deploy security policy for specific Java application, which presents user with window in which he or she can specify the name of the Java application being evaluated, and any parameters the application may require. Also the setting for each of the operation checks defined by the Java security manager class can be specified. The setting is either YES, the operation will be allowed to perform, NO, it will not, or MAYBE it ma[y] be allowed to perform. When this operation is attempted an information window is presented to the user who can decide whether or not to allow the operation.
>
> USE – Allows use to create and deploy security policy for specific Java application.
>
> ADVANTAGE – Allows user to give each application a different level of authorization to controlled actions such as reading and writing the workstation's local storage device.

Like the claims above, this set of claims all recite that "the security modification is a predetermined event indicative of an attempt to circumvent a security mechanism". Applicants have discussed above that this recitation is not shown in *O'Toole*. It is further submitted that as evidenced by the abstract above, which comprises almost the entirety of the cited document, neither does *IBMC* disclose this recited element. Since neither *O'Toole* nor *IBMC* teach or suggest this recitation, their combination is unable to suggest this either.

[10] Office Action dated December 3, 2003, page 4-6.

Moreover, there is no teaching or suggestion in either of *O'Toole* or *IBMC* regarding the desirability of combining these two systems in the manner alleged by the Office Action. Both *O'Toole* and *IBMC* are directed toward very different problems. *O'Toole* changes the permissions granted in a centrally controlled ACL list while *IBMC* controls the behavior for a specific Java application. There is no teaching or suggestion in *O'Toole* to the effect that it would be desirable to controls the behavior for a specific Java application. Moreover, there is no teaching or suggestion in *IBMC* regarding the desirability to changes the permissions granted in a centrally controlled ACL list. Thus, the only teaching or suggestion to even attempt to combine *O'Toole* and *IBMC* is obtained from Applicants' own disclosure and is completely based on a hindsight reconstruction having first had benefit of the knowledge of Applicants' claimed invention and disclosure.

Thus, neither *O'Toole* nor *IBMC*, either alone or in combination, teach or suggest the feature of an instance of a security manager class that determines that a security modification is a notification event if the security modification is a predetermined event indicative of an attempt to circumvent a security mechanism of the trusted computing installation, as recited in representative claim 9. Accordingly, Applicants respectfully request the Appeal Board to withdraw the rejection of claims 9, 10-11, 13, 14 and 15-21 under 35 U.S.C. § 103(a).

Claim 19

It is submitted that claim 19 contains additional limitations that are not shown by the other claims in this grouping and will be argued separately. Claim 19 recites,

> 19. (Previously presented) A trusted computing base, comprising:
> untrusted code executing in the trusted computing base;
> means operative as the untrusted code is executed for determining whether a given security modification has occurred, wherein the given security modification is a predetermined event indicative of an attempt to circumvent a security mechanism of the trusted computing base;
> means responsive to the occurrence of the given security modification for invoking a security notification manager class that issues a given notification. (emphasis added)

As in claim 6, discussed above, claim 19 recites, "untrusted code executing in the trusted computing base". In this claim, it is when untrusted code is running that the "means … for determining" makes its determination regarding security modifications. As discussed above, the application discusses a difference between trusted code and un-trusted code. The user is not physically prevented from running un-trusted code, but is relied on to make a judgment call. If the user chooses to run the code anyway, then it is at this point that notification of the authority is performed. Neither *O'Toole* nor *IBMC* are discussing the use of untrusted code, with its need for letting higher authorities know if a security modification occurs. *O'Toole*, as discussed above, clearly uses trusted code only. Thus, the recitations of claim 19 are not met; the Appeals Board is requested to withdraw the rejection of this claim.

C. **GROUND OF REJECTION 3 (Claim 2)**

The Office Action rejects claim 2 under 35 U.S.C. § 103(a) as being unpatentable over *O'Toole* in view of *Renaud et al.* (U.S. Patent Number 5,958,051), hereinafter referred to as *Renaud*. This rejection is respectfully traversed.

Claim 2 recites,

> 2. The method as described in Claim 1 wherein the predetermined event is chosen from the group consisting of a failed applet signature verification, an addition of a certificate in a certificate database and a modification of a certificate in a certificate database.

The rejection states,

> Referring to claim 2, ... O'Toole teaches addition of the ticket to the access control list, which meets "addition of the certificate in a certificate database". O'Toole, however, does not explicitly teach the notification in the form of applet signature. Renaud discloses implementing digital signatures for data streams (see abstract). Renaud teaches computer-implemented method for verifying the authenticity of data wherein when the data file comprises an applet, and when the signature is not verified, the method includes determining whether an unsigned data file is acceptable for execution on the computer, and terminating the applet if an unsigned data file is not acceptable for execution on said computer (see Fig. 6 and column 17, lines 3-9). Therefore, at the time the invention was made it would have been obvious to one of ordinary skill in the art to send the notification of the security modification to the central authority of O'Toole in the form of failed applet signature as taught in Renaud. One of ordinary skill in the art would have been motivated to send the notification of the security modification to the central authority in the form of failed applet signature as taught in Renaud for determining whether to allow or disallow applet action (see Renaud, Fig. 6, blocks 618 and 620).

Since claim 2 depends from independent claim 1, the same distinctions between *O'Toole* and the invention recited in claim 1 apply to dependent claim 2. In addition, *Renaud* does not provide for the deficiencies of *O'Toole* with regard to independent claim 1. *Renaud* does not teach or suggest the feature of determining that a security modification is a notification event if the security modification is a predetermined event indicative of an attempt to circumvent a security mechanism of a trusted computing installation, as recited in claim 1. Thus, any alleged combination of *Renaud* with *O'Toole* still would not result in the invention recited in claim 1, from which claim 2 depends.

Regarding the specific recitations of claim 2, the rejection as cited above has rather blithely equated the "addition of the ticket to the access control list" to the "addition of the certificate in a certificate database". If the words of a claim are to have any meaning, then it is proper to make such a substitution only if the two actions would be seen to create equivalent ends. Yet, it is submitted that one of ordinary skill in the art would not consider adding a ticket to an access control list as equivalent to adding a certificate to a certificate database. While both the access control list and the certificate database are related to security, they are two different items and adding a new entry to each would reach different ends. The access control list allows access to a computer system to trusted individuals or services; a certificate database contains certificates by which messages purported to be from given individuals can be verified as actually being from those individuals. Thus, it is submitted, these actions are not the same.

Additionally, *Renaud* is directed toward implementing digital signatures for data streams and data archives and it appears that the office action cites *Renaud* solely as demonstrating this capability. *Renaud* does not provide any other teaching or suggestion that would cause one of ordinary skill to use this event as a trigger to send a notification to higher authorities, as recited in the claim, such as using a failed signature verification as a trigger for a notification to the authorities. Thus, both by virtue of its dependency on claim 1 and its own unique recitations, claim 2 is distinguished over the alleged combination of *O'Toole* and *Renaud.* Accordingly, Applicants respectfully requests the Appeal Board to withdraw the rejection of claim 2 under 35 U.S.C. § 103(a).

D. <u>GROUND OF REJECTION 4 (Claims 3 and 12)</u>

The Office Action rejects claims 3 and 12 under 35 U.S.C. § 103(a) as being obvious over *O'Toole* in view of *IBMC* and *Renaud.* This rejection is respectfully traversed.

Representative claim 3 recites,

> 3. (Previously presented) The method as described in Claim 1 wherein the predetermined event is created by a Java applet wishing to run with higher privileges and further comprising the steps of:
> verifying a signature of the Java applet;
> responsive to a failed verification of the signature, running the applet as untrusted; and
> sending the central authority a notification of the failed verification.

Since representative claim 3 depends from independent claim 1, the same distinctions over *O'Toole* exist and apply to dependent claim 3. In addition, as discussed above with regard to claim 2, *Renaud* does not provide for the deficiencies of *O'Toole* with regard to independent claim 1. *Renaud* does not teach or suggest the feature of determining that a security modification is a notification event if the security modification is a predetermined event indicative of an attempt to circumvent a security mechanism of the trusted computing installation, as recited in claim 1. Likewise, as discussed with regard to claim 9 above, *IBMC* does not provide for the deficiencies of claim 1 and does not teach this feature. Thus, any alleged combination of *Renaud* and *IBMC* with *O'Toole* still would not result in the invention recited in claim 1, from which claim 3 depends.

Further, while *Renaud* teaches "wherein when the data file comprises an applet, and when the signature is not verified, the method includes determining whether an unsigned data file is acceptable for execution on the computer, and terminating the applet if an unsigned data file is not acceptable for execution on said computer"[11], this patent does not appear to disclose that if the user allows an untrusted applet to run, then a notification should be sent to the higher authorities, advising them of this possible problem.

Therefore, both by virtue of its dependency on claim 9 and its own unique recitation, claim 3 defines over the alleged combination of *O'Toole*, *IBMC* and *Renaud*. Accordingly, Applicants respectfully request the Board of Appeals to withdraw the rejection of these claims under 35 U.S.C. § 103(a).

[11] Renaud, claim 13, column 17, lines 3-10.

CONCLUSION

It is submitted that all claim rejections should be overturned for the reasons discussed above. The Board of Appeals is requested to reverse the rejections and allow this application.

Betty Formby

Betty G. Formby
Reg. No. 36,536
YEE & ASSOCIATES, P.C.
PO Box 802333
Dallas, TX 75380
(972) 385-8777

CLAIMS APPENDIX

The text of the claims that are involved in the appeal reads:

1. A method for notifying a central authority of changes to a trusted computing installation, comprising the steps of:

determining that a user has made a security modification to a portion of the trusted computing installation under user control;

determining that the security modification is a notification event if the security modification is a predetermined event indicative of an attempt to circumvent a security mechanism of the trusted computing installation; and

sending the central authority a notification of the security modification, in response to determining that the security modification is a notification event.

2. The method as described in Claim 1 wherein the predetermined event is chosen from the group consisting of a failed applet signature verification, an addition of a certificate in a certificate database and a modification of a certificate in a certificate database.

3. The method as described in Claim 1 wherein the predetermined event is created by a Java applet wishing to run with higher privileges and further comprising the steps of:

verifying a signature of the Java applet;

responsive to a failed verification of the signature, running the applet as untrusted; and

sending the central authority a notification of the failed verification.

4. The method as described in Claim 1 wherein the central authority provides a mechanism wherein the group of predetermined events can be modified by an authorized user.

5. The method as described in Claim 1 wherein the notification is chosen from the group consisting of an SNMP alert, an e-mail, a screen message and an online database.

6. The method as described in Claim 1 wherein the security modification is to allow untrusted code to run in the trusted computing installation.

7. The method as described in Claim 1 wherein the step of determining that the security modification is a notification event is accomplished by an abstract class instantiation which defines the type of notification in a concrete implementation of the abstract class instantiation.

8. The method as described in Claim 1 wherein the trusted computing installation further comprises a Java Virtual Machine resident in a local machine under user control.

9. A method of notifying a central authority of changes to a trusted computing installation, comprising the steps of:

determining that a user has made a security modification to a portion of the trusted computing installation under user control;

invoking a security notification manager class;

instantiating the security manager class with an instance that determines that the security modification is a notification event if the security modification is a predetermined event indicative of an attempt to circumvent a security mechanism of the trusted computing installation; and

sending the central authority a notification of the security modification, in response to determining that the security modification is a notification event.

10. The method as described in Claim 9 wherein the notification is selected from a group of notifications consisting of: an SNMP alert, an e-mail, a database log, and a screen message.

11. The method as described in Claim 9 wherein the determining step executes a given control routine when the user has made a security modification to a portion of the trusted computing installation under user control.

12. The method as described in Claim 11 wherein the portion of the trusted computing installation is an applet signature verification routine.

13. The method as described in Claim 11 wherein the portion of the trusted computing installation is a certificate modification routine.

14. A method for notifying a central authority of changes to a trusted computing installation, comprising the steps of:

upon a given security modification, invoking a security notification manager class;

extending the security notification manager class with one of a set of instances, wherein a given instance determines that the security modification is a notification event if the security modification is a predetermined event indicative of an attempt to circumvent a security mechanism of the trusted computing installation, and

sending the central authority a notification of the security modification, in response to determining that the security modification is a notification event.

15. A computer program product in a computer-useable medium for notifying an authority of changes to a trusted computing installation, comprising:

a security notification manager class;

at least one class instance for the security notification manager class for determining that a given security modification is a notification event if the security modification is a predetermined event indicative of an attempt to circumvent a security mechanism of the trusted means for sending the authority a notification of the given security modification in response to determining that the security modification is a notification event.

16. The computer program product as described in Claim 15 wherein the notification is selected from a group of notifications consisting of: an SNMP alert, an e-mail, a database log, and a screen message.

17. The computer program product as described in Claim 15 further including a control routine for determining when the user has made a security modification to a portion of the trusted computing installation to generate the given security modification.

18. A computer program product in a computer-readable medium for notifying an authority of changes to a trusted computing installation, comprising:

a control routine executed upon a given security modification in the trusted computing installation for invoking an abstract Java class;

at least one class instance for the abstract Java class for determining that the given security modification is a notification event if the security modification is a predetermined event indicative of an attempt to circumvent a security mechanism of the trusted computing installation; and

means for sending the authority a notification of the given security modification in response to determining that the security modification is a notification event.

19. A trusted computing base, comprising:

untrusted code executing in the trusted computing base;

means operative as the untrusted code is executed for determining whether a given security modification has occurred, wherein the given security modification is a predetermined event indicative of an attempt to circumvent a security mechanism of the trusted computing base;

means responsive to the occurrence of the given security modification for invoking a security notification manager class that issues a given notification.

20. The trusted computing base as described in Claim 19 further including a set of one or more security notification manager class instances, wherein a given security notification manager class instance extends the security notification manager class to identify a given security modification.

21. The trusted computing base as described in Claim 20 wherein a given security manager class instance includes at least first and second rules, wherein the first rule triggers a first notification and the second rule triggers a second notification.

22. A notification service for a trusted computing installation, comprising:

a pluggable framework for receiving a set of notification objects, wherein each notification objects identifies a given notification that is issued upon a given security modification to the trusted computing installation, wherein the given security modification is a predetermined event indicative of an attempt to circumvent a security mechanism of the trusted computing base; and

means for issuing the given notification upon the occurrence of its associated security modification.

23. The notification service as described in Claim 22 wherein the given notification is selected from a group of notifications consisting of: an SNMP alert, an e-mail, a database log, and a screen message.